(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 503 040**

(51) Int. CI.:

G06F 21/00 (2013.01)
H04L 29/06 (2006.01)
H04L 12/24 (2006.01)
H04L 12/28 (2006.01)
G06F 21/31 (2013.01)
H04L 29/08 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **21.10.2010 E 10766297 (5)**

(97) Fecha y número de publicación de la concesión europea: **23.07.2014 EP 2517137**

(54) Título: **Procedimiento y dispositivo para asegurar la comunicación entre un servidor de domótica y un servidor de configuración central**

(30) Prioridad:

22.12.2009 DE 102009060469

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
06.10.2014

(73) Titular/es:

RWE EFFIZIENZ GMBH (50.0%)
Flamingoweg 1
44139 Dortmund, DE y
EQ-3 AG (50.0%)

(72) Inventor/es:

DANKE, ENNO y
GROHMANN, BERND

(74) Agente/Representante:

VEIGA SERRANO, Mikel

DESCRIPCIÓN

Procedimiento y dispositivo para asegurar la comunicación entre un servidor de domótica y un servidor de configuración central

Sector de la técnica

El objeto se refiere a un procedimiento para generar una autorización de acceso a un servidor de automatización por medio de un servidor de configuración central a través de una red de área amplia. Además, el objeto se refiere a un servidor de domótica así como a un servidor de configuración central, así como a un sistema con servidores de este tipo.

Estado de la técnica

Se conocen suficientemente sistemas para domótica. Así se conoce, por ejemplo, bajo la denominación EIB/KNX un sistema domótico por cable, en el que a través de un bus en serie se intercambian mensajes entre sensores y actuadores y de manera correspondiente a reglas que pueden fijarse (parámetros) se controlan dispositivos consumidores eléctricos. Sin embargo, un sistema de bus de este tipo requiere un cableado complejo, que puede realizarse casi exclusivamente en nueva construcción.

También se conoce un sistema para domótica por la publicación WO-A1-2009/129821.

Además de la comunicación entre sí, es decir entre los aparatos (actuadores, sensores) y el servidor de domótica (servidor de domótica) también debe protegerse la comunicación con un servidor de configuración central frente a ataques por terceros. Así, debe garantizarse que en cada caso sólo el propietario actual del servidor de domótica tenga acceso al servidor de domótica a través de una red de área amplia.

Objeto de la invención

Por tanto, el objeto se basó en el objetivo de poner a disposición una relación de propiedad segura entre un servidor de domótica y un usuario en un servidor de configuración central. Además, en el caso de un traspaso de propiedad del servidor de domótica, el propósito era poner a disposición una comunicación todavía segura entre el nuevo propietario y el servidor de domótica.

Este objetivo se alcanza según el objeto según un primer aspecto mediante un procedimiento para generar una autorización de acceso a un servidor de domótica por medio de un servidor de configuración central a través de una red de área amplia, que comprende almacenar al menos una primera tupla formada por un identificador que identifica unívocamente el servidor de domótica y un código de registro en el servidor de configuración central, recibir una segunda tupla formada por al menos un identificador y un código de registro en el servidor de configuración central de un usuario, comparar la primera tupla con la segunda tupla mediante el servidor de configuración central, almacenar una relación de propiedad entre el usuario y el servidor de domótica en caso de un resultado de comparación positivo, de tal manera que por medio de la relación de propiedad se genera una autorización de acceso al servidor de domótica a través de la red de área amplia.

La autorización de acceso al servidor de domótica a través de la red de área amplia puede generarse por medio del servidor de configuración central o del servidor de domótica, en particular mediante la emisión de una orden correspondiente en caso de existir una autorización de acceso y/o mediante el bloqueo de la comunicación en caso de no existir autorización de acceso. La autorización de acceso (autenticación) puede producirse con respecto al servidor de configuración o el servidor de domótica o ambos.

Cuando la autorización de acceso sólo está almacenada en una ubicación, la en cada caso una ubicación puede remitir una solicitud de autenticación a la en cada caso otra ubicación.

La relación de propiedad entre el usuario y el servidor de domótica puede almacenarse en el ordenador de configuración central o el servidor de domótica.

Para una puesta en marcha sencilla de un servidor de domótica (*Smart Home Server*, SHC), el usuario del servidor de domótica debe poder establecer de manera sencilla, por ejemplo a través de Internet, por ejemplo mediante la conexión a un encaminador DSL, una conexión entre el servidor de domótica y un servidor de configuración central. A través de esta conexión, el usuario debe poder configurar de manera muy sencilla, por ejemplo a través de una página web, el servidor de domótica. Para ello, entre el servidor de domótica y el servidor de configuración central se establece a través de Internet una conexión de configuración. Esta conexión puede producirse, por ejemplo, a través de un túnel de IP. También es posible que se establezca una conexión VPN entre el servidor de domótica y el servidor de configuración.

Por un lado, la conexión debe estar asegurada como tal y, por otro lado, también debe estar asegurado el acceso del servidor de configuración central al servidor de domótica. En particular, ante el trasfondo de que el acceso al servidor de configuración y desde éste entonces al servidor de domótica se produce a través de una red de área amplia, por ejemplo Internet, hay que partir de que existe un elevado potencial de amenaza, dado que un tercero puede intentar “capar” la conexión con el servidor de domótica para configurar entonces el servidor de domótica.

Por tanto, para una configuración a través de la red de área amplia es necesario que el usuario se autentique frente al servidor de configuración central y/o al servidor de domótica. En particular en el caso de una primera instalación, o en el caso de reiniciar el servidor de domótica al estado de entrega, es necesario un registro del usuario y el servidor de domótica en el servidor de configuración central.

Según el objeto se propone que sólo se permita a usuarios autenticados el uso y/o la configuración del servidor de domótica a través de la red de área amplia por medio del servidor de configuración. Para ello es necesario que en primer lugar tenga que configurarse una relación de propiedad entre el usuario y el servidor de domótica. A este respecto, la configuración se produce preferiblemente en el servidor de configuración central. La configuración satisfactoria de una relación de propiedad puede almacenarse en el servidor de configuración central y/o el servidor de domótica. Con ayuda de esta relación de propiedad el usuario puede acceder entonces a través del servidor de configuración al servidor de domótica asociado al mismo y realizar configuraciones.

Además, debe ser posible crear, por medio de la relación de propiedad configurada antes, perfiles de usuario, que pueden presentar diferentes posibilidades de acceso y restricciones en el servidor de domótica.

Se ha reconocido que para configurar una relación de propiedad es necesaria una autenticación. En esta autenticación, el usuario debe demostrar según el objeto además del conocimiento también la propiedad del servidor de domótica con respecto al servidor de configuración. Esto significa que según el objeto son necesarios dos factores para la autenticación.

Un factor es un factor de conocimiento. Según el objeto, este factor de conocimiento es el identificador que identifica unívocamente el servidor de domótica. Una vez que un usuario está en posesión de un servidor de domótica, puede averiguar este identificador y por consiguiente tiene el conocimiento. Para el primer propietario del servidor de domótica, el factor de conocimiento representa una protección suficiente frente a terceros. Sin embargo, al traspasar el servidor de domótica este conocimiento sigue estando en el usuario anterior y además en el nuevo usuario. Por consiguiente se distribuye el conocimiento a todos los propietarios del servidor de domótica. Esto conduce a que el factor de conocimiento no ofrezca una protección suficiente frente a que propietarios anteriores del servidor de domótica tras su reinicio al estado de entrega lo autoricen para sí mismos y el nuevo propietario ya no pueda realizar la autorización.

Para posibilitar también en el caso de un traspaso del servidor de domótica una autenticación segura, es necesario que además del factor de conocimiento se use un factor de propiedad. Según el objeto, el factor de propiedad es el código de registro. El código de registro es según el objeto un código, que sólo se da a conocer al propietario actual del servidor de domótica. Esto significa que el código de registro según el objeto se visualiza exclusivamente en el servidor de domótica al propietario actual. Sin embargo, esto también significa que el código de registro se modifica, en la medida en que éste sólo se mantiene igual como máximo hasta el traspaso del servidor de domótica y después se modifica obligatoriamente. Por consiguiente, a más tardar con el traspaso del servidor de domótica se genera de nuevo el factor de propiedad, el antiguo propietario ya no lo conoce y sólo el nuevo propietario puede autorizarse de nuevo.

La autorización requiere una relación de propiedad entre el usuario y el servidor de domótica. Esta relación de propiedad puede estar protegida a través de una contraseña y un nombre de usuario. A la contraseña y al nombre de usuario puede asociarse una clave de comunicación unívoca, con cuya ayuda se asegura la comunicación entre el servidor de comunicación central y el servidor de domótica. Por medio del nombre de usuario y de la contraseña puede estar asegurado el acceso al servidor de domótica a través del servidor de configuración o dentro de una red local en la que está integrado el servidor de domótica. La relación de propiedad garantiza que un usuario puede asegurar un acceso al servidor de domótica, sin que un tercero pueda realizar un acceso no autorizado al servidor de domótica.

Según un ejemplo de realización ventajoso se propone que el código de registro sea un código aleatorio generado en el servidor de domótica, por ejemplo en un módulo de plataforma de confianza (*Trusted Platform Module*), y que la primera tupla se transmita desde el servidor de domótica al servidor de configuración central preferiblemente de manera cifrada a través de la red de área amplia. Por ejemplo, tras establecer la alimentación con tensión del servidor de domótica, cuando todavía no existe ninguna relación de propiedad, o tras reiniciar el servidor de domótica al estado de entrega puede generarse un código aleatorio, por ejemplo un código de símbolos, un código de cifras o un código de números. Esto puede producirse con ayuda de un generador de números aleatorios.

También es posible que el código de registro se genere en el servidor de configuración. Esto es posible, por ejemplo, siempre que un servidor de domótica indique con respecto al servidor de configuración a través de la red de área

amplia, que éste se ha reiniciado al estado de entrega. A través de un canal asegurado, el servidor de configuración puede transmitir entonces el código de registro generado en el mismo al servidor de domótica. El tipo del código de registro así como la generación del código de registro puede ser en el servidor de configuración igual a como se describe para el servidor de domótica.

Por consiguiente, se propone que el código de registro sea un código aleatorio generado en el servidor de configuración central y que el código de registro se transmita desde el servidor de configuración central al servidor de domótica a través de la red de área amplia. También es posible que el código de registro sea una combinación de códigos aleatorios generados en el servidor de configuración central y en el servidor de domótica y que los códigos aleatorios se intercambien entre el servidor de configuración central y el servidor de domótica a través de la red de área amplia. En este caso, el código de registro es especialmente seguro, dado que se compone de dos códigos aleatorios generados por separado uno de otro.

Una vez que se ha generado un nuevo código de registro, éste puede transmitirse junto con el identificador que identifica unívocamente el servidor de domótica al servidor de configuración central. La transmisión debe estar igualmente asegurada, dado que de lo contrario el código de registro podría interceptarse. Esta transmisión puede asegurarse por medio de claves almacenadas de manera fija en el servidor de domótica y el servidor de configuración. El cifrado puede ser tanto simétrico como asimétrico. Una vez que el servidor de configuración recibe una tupla de este tipo, la descifra y almacena.

Si un usuario quiere establecer ahora una relación de propiedad con el servidor de domótica, en primer lugar puede comunicar el identificador unívoco por medio de, por ejemplo, una interfaz de usuario a través de un navegador (interfaz web) al servidor de configuración. El servidor de configuración busca en su memoria el identificador unívoco y el código de registro asociado que se recibió previamente.

El usuario debe introducir ahora además del identificador unívoco también el código de registro. Dado que el código de registro se genera de nuevo al menos para cada nuevo propietario, sólo el propietario actual puede conocer el código de registro. Por consiguiente se garantiza que un propietario anterior no pueda establecer ninguna nueva relación de propiedad. El nuevo propietario se entera del código de registro por el servidor de domótica y lo comunica junto con el identificador al servidor de configuración central. Si los datos del usuario coinciden con los datos almacenados, entonces se establece una relación de propiedad entre el usuario y el servidor de domótica.

Esta relación de propiedad puede asegurarse mediante un nombre de usuario y una contraseña. Tras introducir satisfactoriamente el código de registro ya sólo se produce la autenticación mediante nombre de usuario/contraseña, es decir mediante el conocimiento del nuevo propietario, que el anterior propietario no puede saber. Por medio de esta relación de propiedad se produce una autorización de acceso a través del servidor de configuración al servidor de domótica. El usuario puede configurar entonces el servidor de domótica por medio del servidor de configuración, por ejemplo por medio de un servicio basado en Internet.

El código de registro, según un ejemplo de realización ventajoso, puede presentarse visualmente al usuario mediante un dispositivo de visualización en el servidor de domótica. El dispositivo de visualización puede ser una pantalla. El dispositivo de visualización puede ser una pantalla de 8 cifras de 15 segmentos. El dispositivo de visualización puede ser también una pantalla TFT. El dispositivo de visualización puede ser también una pantalla OLED. Un dispositivo de visualización de este tipo o también otros posibilitan la reproducción del código de registro generado en el servidor de domótica. El propietario actual puede leer el código de registro a través del dispositivo de visualización y puede transmitirse junto con el identificador al servidor de configuración.

Tal como ya se explicó anteriormente, según un ejemplo de realización ventajoso se propone que en cada caso se genere un nuevo código de registro cada vez que se reinicie el servidor de domótica y que la primera tupla formada con ello se transmita desde el servidor de domótica al servidor de configuración central a través de la red de área amplia. Por consiguiente, cada vez que se reinicia el servidor de domótica se deposita en el servidor de configuración una nueva tupla, con cuya ayuda puede establecerse la relación de propiedad. La tupla almacenada anteriormente puede borrarse o hacerse inactiva. El código de registro también puede pasar a ser inactivo o no válido con el almacenamiento de una relación de propiedad entre el usuario y el servidor de domótica. Así es posible, por ejemplo, cuando el usuario se registra en el servidor de configuración con ayuda de la segunda tupla y existe un resultado de comparación positivo entre la primera tupla y la segunda tupla, que el código de registro pase entonces a ser no válido. Así se garantiza que en cada caso sólo sea posible un registro único con un código de registro generado antes.

Según un ejemplo de realización ventajoso se propone que al código de registro esté asociado un periodo de validez y que tras la expiración del periodo de validez sea imposible generar una autorización de acceso con el código de registro caducado. Por un lado, es posible que la visualización del nuevo código de registro creado sólo se produzca durante cierto tiempo en la pantalla. Por consiguiente, el propietario sólo puede leer el código de registro poco después de reiniciar el servidor de domótica. Después tiene que o bien recordarlo o bien reiniciar de nuevo el servidor de domótica. En el servidor de configuración central puede estar establecido un mecanismo, que marca la tupla almacenada como válida sólo durante cierto tiempo. Tras la expiración de este tiempo se marca la tupla como

no válida e incluso en caso de introducir una tupla correcta puede rechazarse la creación de la relación de propiedad mediante el servidor de configuración. Tras establecer la relación de propiedad el código de registro puede pasar igualmente a ser no válido, es decir entonces sólo puede usarse una vez.

La relación de propiedad posibilita la creación de cuentas de usuario. Las cuentas de usuario posibilitan definir diferentes autorizaciones de acceso al servidor de domótica. Por este motivo se propone que con ayuda de una autorización de acceso se cree una cuenta de usuario, pudiendo estar asociadas a una cuenta de usuario restricciones de acceso al servidor de domótica. Por consiguiente, por medio de las cuentas de usuario pueden crearse diferentes perfiles de usuario y perfiles de autorización de acceso.

Según un ejemplo de realización ventajoso se propone que la cuenta de usuario se almacene en el servidor de domótica y/o el servidor de configuración central. Por consiguiente, las diferentes cuentas de usuario pueden estar depositadas en los diferentes servidores.

Según un ejemplo de realización ventajoso, el identificador es un número de serie del servidor de domótica. Este identificador representa por consiguiente el conocimiento, que puede quedar en cada propietario del servidor de domótica y al mismo tiempo identifica unívocamente el servidor de domótica.

Para evitar que el identificador junto con el código de registro, en caso de la generación del código de registro, deba transmitirse desde el servidor de domótica al servidor de configuración central, lo que representa un punto de ataque, se propone también que el código de registro sea un código variable generado en el servidor de domótica.

También es posible transmitir el código como código *hash* en lugar de una transmisión como texto claro.

También es posible, por ejemplo, almacenar un número limitado de códigos, varios miles, varias decenas de miles, varios millones, en una memoria tanto en el servidor de domótica como en el servidor de configuración central. Una vez que se ha llamado un código de registro en el servidor de domótica, un contador salta automáticamente al siguiente valor, lo que significa que en la siguiente llamada se usará el siguiente código de registro almacenado. Lo mismo tiene lugar en el servidor de comunicación, cuando un usuario intentar usar el identificador junto con el código de registro para crear una relación de propiedad. Por consiguiente, tanto en el servidor de domótica como en el servidor de configuración central están depositadas listas, que contienen los códigos de registro correspondientes.

Un aparato puede ser un sensor y/o un actuador.

Un sensor puede ser, por ejemplo, un conmutador, un detector de movimiento, un pulsador, un contacto de puerta, un termostato, un contacto de ventana, un sensor de imágenes, un sensor de claridad, un sensor de temperatura, un sensor binario, un micrófono u otra unidad para detectar variaciones del entorno.

Un actuador puede ser, en particular, un relé, una válvula, un motor, un servomotor, un regulador de luz, un control de persiana, un conmutador, un transmisor de señales, un transmisor de señales de infrarrojos, un transmisor de señales acústico, un dispositivo de mando, un terminal de información u otro aparato para realizar operaciones de conmutación, operaciones de control, operaciones de regulación u otras acciones y/o para emitir información y estados.

Un servidor de domótica (aparato de control central, *Smart Home Controller*, SHC) puede ser un ordenador dispuesto de manera central, que adopta funciones de control. Éste puede procesar y emitir parámetros para la configuración de sensores y actuadores. El servidor también puede estar encargado de la gestión central de claves de comunicación. En particular, el servidor puede ser responsable de una puesta en conocimiento central de una clave de red. El servidor puede estar conectado, por ejemplo, con una red de área amplia. A este respecto, es posible, por ejemplo, que el servidor esté conectado a través de un encaminador correspondiente con una red de área amplia, por ejemplo una red de área amplia basada en TCP/IP. En particular, puede ser posible acceder al servidor de domótica por medio de un servidor de configuración a través de la red de área amplia y realizar configuraciones de manera remota. El servidor puede ser de tal manera que únicamente se comunique con fines de configuración con los sensores y los actuadores. Además, el sistema domótico puede estar diseñado de tal manera que se produzca una comunicación entre los sensores y los actuadores para el control en reacción a acontecimientos, sin que el servidor esté interconectado. De este modo puede realizarse una domótica autárquica, que también funciona sin un servidor. Sin embargo, esto sólo es posible de manera segura cuando se conoce una clave de red para el cifrado de la comunicación en los aparatos.

El procesador puede ser, por ejemplo, un procesador de señales digitales (DSP). El procesador también puede ser un microcontrolador. El procesador puede ser cualquier microcontrolador que esté configurado por un lado para evaluar señales de entrada y por otro lado para emitir señales de control.

Las interfaces de comunicación pueden ser, por ejemplo, unidades para la comunicación a través de una red inalámbrica. Una interfaz de comunicación también puede comunicarse a través de una red por cable. Por ejemplo puede producirse una comunicación a través de LAN, WLAN, *Bluetooth* o similares. En particular, la interfaz de

comunicación, por ejemplo a una frecuencia de 868 Mz, puede emitir mensajes con un desplazamiento de frecuencia. En particular son posibles tasas de transmisión de datos de 10 KB/s. Un protocolo de acceso puede ser, por ejemplo, un protocolo de acceso CSMA/CA.

La comunicación por medio de la segunda interfaz de comunicación puede ser una comunicación bidireccional en un bus, en particular un bus de radio. La interfaz de comunicación puede estar configurada para el cifrado de los datos transmitidos. En particular, un cifrado simétrico puede estar soportado por la interfaz de comunicación. En particular, puede estar soportado un cifrado CCM o cifrado CCM*. En particular puede usarse un procedimiento de cifrado autenticado según la norma IEEE 802.11. También es posible un procedimiento de cifrado ampliado según la norma de encriptación avanzada, modo de recuento (*Advanced Encryption Standard Counter Mode*, AES/CCM), en el que se usa un cifrado por bloques de 16 bytes. Para el cifrado simétrico puede ser posible que cada sensor, cada actuador y cada ordenador de control central (servidor) presente un número de serie. También puede ser posible que el número de serie de cada aparato sea conocido para una central. La comunicación a través de la interfaz de comunicación puede producirse en el modo de multidifusión así como de unidifusión.

Un aspecto adicional es un servidor de domótica con un procesador, una primera interfaz de comunicación para la comunicación a través de una red de área amplia con un servidor de configuración central, una segunda interfaz de comunicación para la comunicación con aparatos locales y una unidad de visualización, que se caracteriza porque el procesador activa la unidad de visualización para visualizar un código de registro y porque el procesador para configurar una autorización de acceso a través de la red de área amplia al servidor de domótica activa la primera interfaz de comunicación para emitir el código de registro junto con un identificador que identifica unívocamente el servidor de domótica al servidor de configuración central.

El código de registro puede generarse también en el servidor de configuración central y recibirse por el servidor de domótica y presentarse visualmente al usuario. El identificador que identifica unívocamente el servidor de domótica puede almacenarse en el servidor de configuración central junto con el código de registro generado en el mismo. Un usuario puede establecer una relación introduciendo en el servidor de configuración central el código de registro junto con el identificador que identifica unívocamente el servidor de domótica y demostrando por consiguiente la propiedad del servidor de domótica. Entonces puede suprimirse una transmisión del código de registro junto con el identificador que identifica unívocamente el servidor de domótica desde el servidor de domótica al servidor de configuración central, dado que en el servidor de configuración central ya se conoce el código de registro y éste está asociado unívocamente al identificador que identifica el servidor de domótica.

También es posible que el código de registro se componga de códigos aleatorios, que se generaron por un lado en el servidor de domótica y por otro lado en el servidor de configuración central. Los códigos aleatorios pueden combinarse en el servidor de domótica y en el mismo puede generarse el código de registro. También es posible que los códigos aleatorios se combinen en el servidor de configuración central.

También puede estar prevista una memoria para almacenar una relación de propiedad entre el usuario y el servidor de domótica en el servidor de configuración central en caso de un resultado de comparación positivo en el servidor de domótica.

Un aspecto adicional es un servidor de configuración central con una memoria configurada para almacenar al menos una primera tupla formada por un identificador que identifica unívocamente el servidor de domótica y un código de registro en el servidor de configuración central, una interfaz de comunicación configurada para recibir una segunda tupla formada por al menos un identificador y un código de registro en el servidor de configuración central de un usuario, un procesador configurado para comparar la primera tupla con la segunda tupla, posibilitando la interfaz de comunicación con ayuda de la relación de propiedad un acceso al servidor de domótica a través de la red de área amplia.

La memoria puede estar configurada para almacenar una relación de propiedad entre el usuario y el servidor de domótica en el servidor de configuración central en caso de un resultado de comparación positivo.

Un aspecto adicional es un sistema con un servidor de configuración central de este tipo y un denominado servidor de domótica.

Los procedimientos mencionados anteriormente también pueden realizarse como programa informático o como programa informático almacenado en un medio de almacenamiento. A este respecto, en el lado del sensor, el lado del actuador y/o el lado del servidor puede estar programado de manera adecuada un microprocesador para realizar las respectivas etapas de procedimiento mediante un programa informático.

Las características de los procedimientos y dispositivos pueden combinarse libremente entre sí. En particular, las características de las reivindicaciones dependientes pueden ser inventivas por sí mismas individualmente o combinadas libremente entre sí evitando las características de las reivindicaciones independientes.

Descripción de las figuras

A continuación se explica más detalladamente el objeto mediante un dibujo que muestra ejemplos de realización.

En el dibujo muestran:

la figura 1 un ejemplo de realización de un sistema para domótica;

la figura 2 una vista esquemática de un servidor de domótica;

la figura 3 una vista esquemática de un servidor de comunicación central;

la figura 4 un diagrama de flujo a modo de ejemplo según un primer ejemplo de realización;

la figura 5 un diagrama de flujo a modo de ejemplo según un segundo ejemplo de realización;

la figura 6 un diagrama de flujo a modo de ejemplo según un tercer ejemplo de realización.

Descripción detallada de la invención

La figura 1 muestra por ejemplo el entorno (26) de una casa o de un piso. En este entorno (26) está previsto un encaminador (24), que pone a disposición una conexión de comunicación con Internet (28) y puede enviar a Internet (28) y recibir de Internet (28) paquetes de datos. Al encaminador (24) está conectado un servidor (22) de domótica (*Smart Home Controller*, SHC). A través del encaminador (24) el SHC (22) puede intercambiar paquetes de datos con Internet (28). El SHC (22) puede establecer a través de una conexión por radio una comunicación con sensores (2) así como con actuadores (12). La comunicación puede ser bidireccional y producirse a demanda.

A Internet (28) está conectada una unidad (30) de gestión central (servidor de configuración central). La unidad (30) de gestión central puede establecer a través de Internet (28) y el encaminador (24) una comunicación con el SHC (22), para realizar, por ejemplo, una configuración de los sensores (2), de los actuadores (12) o del SHC (22).

La configuración del SHC (22) así como de los sensores (2) y de los actuadores (12) a través de Internet (28) puede producirse, por ejemplo, por un ordenador (32a) personal privado. Para ello, el ordenador (32a) personal puede establecer por ejemplo una conexión a través de Internet (28) con la unidad (30) de gestión central y realizar por medio de la unidad (30) de gestión central una configuración del SHC (22), del sensor (2) o del actuador (12). Esta modificación de la configuración puede transmitirse entonces a través de Internet (28) desde la unidad (30) de gestión central a través del encaminador (24) al SHC (22). También puede producirse una configuración, por ejemplo, a través de un teléfono (32b) móvil, estando conectado el teléfono (32b) móvil a través de una pasarela (34) con Internet (28) y pudiendo establecer a través de la pasarela (34) una conexión con la unidad (30) de gestión central.

Una comunicación segura entre el SHC (22) y la unidad (30) de gestión central puede garantizarse, por ejemplo, porque el SHC (22) establece por medio del encaminador (24) un túnel de comunicación mediante Internet (28) con la unidad (30) de gestión central, una vez que se conecta el SHC (22) con el encaminador (24). Para ello, el SHC (22) únicamente tiene que conocer la dirección IP fija o el nombre DNS de la unidad (30) de gestión central y cifrar por medio de una contraseña y un clave la comunicación con la unidad (30) de gestión central. La autenticación del SHC (22) en la unidad (30) de gestión central puede producirse a través de secreto compartido (*Shared Secret*) o a través de certificados. Para la primera comunicación puede usarse un certificado por defecto. Después, cada SHC puede obtener un certificado “de por vida” personalizado, a través del que es posible una comunicación cifrada segura.

A través de esta conexión cifrada puede producirse ahora desde la unidad (30) de gestión central una configuración del SHC (22), del sensor (2) así como del actuador (12). La configuración puede controlarse por el ordenador (32a) personal o el teléfono (32b) móvil. También es posible generar por medio del ordenador (32a) personal así como del teléfono (32b) móvil acontecimientos en el sensor (2), para desencadenar así determinadas acciones de los actuadores (12). También pueden consultarse de esta manera estados de los sensores (2) y los actuadores (12).

La comunicación entre SHC (22), actuadores (12) y sensores (2) posibilita por un lado la configuración de los sensores (2) y de los actuadores (12) así como el control de dispositivos consumidores eléctricos conectados al actuador (12) por medio de los sensores (2). El control del actuador se regula mediante enlaces entre un sensor (2) y actuadores (12) así como mediante parámetros de sensor y/o parámetros de actuador.

A los diferentes actuadores (12) pueden conectarse los más diversos dispositivos consumidores eléctricos. En la configuración del sensor (2) así como de los actuadores (12) a través del SHC (22) puede reducirse según el objeto la propagación de comunicación con un sensor (2), de modo que el sensor (2) con alimentación de energía propia consuma la menor cantidad de energía posible. Los actuadores (12) pueden alimentarse por ejemplo de manera permanente con energía, por ejemplo estar conectados a una alimentación de energía eléctrica y por consiguiente

recibir y emitir mensajes permanentemente. Los actuadores (12) también pueden estar configurados de tal manera que reciban permanentemente mensajes y emitan mensajes a intervalos. Los actuadores (12) también pueden estar configurados de tal manera que puedan recibir permanentemente mensajes y sólo emitir mensajes a demanda. El ahorro de energía debe producirse principalmente en los sensores (2) que tienen una alimentación de energía propia.

Sin embargo, además del ahorro de energía también es importante asegurar la comunicación y el acceso al SHC (22) por medio del servidor (30) de configuración central.

Para asegurar el acceso al SHC (22), es necesario un SHC previsto en la figura 2. La figura 2 muestra el SHC (22) con una interfaz (22a) de comunicación. La interfaz (22a) de comunicación sirve para la comunicación a través del encaminador (24) con Internet (28) y por consiguiente entre el SHC (22) y el servidor (30) de configuración central.

Además está previsto un procesador (22b) central, que activa los componentes individuales del SHC (22). Además, el SHC (22) presenta una memoria (22c), en la que pueden almacenarse cuentas de usuario. Además pueden estar almacenadas reglas y parámetros de sensor y de actuador para controlar el sistema domótico. El SHC (22) presenta además una segunda interfaz (22d) de comunicación, con la que es posible una comunicación con los actuadores (12) y los sensores (2), preferiblemente de manera inalámbrica.

Finalmente, el SHC (22) presenta un dispositivo (22e) de visualización, a través del que puede presentarse visualmente un código de registro a un usuario. En cada nuevo inicio del SHC (22) o al reiniciar cada vez el SHC (22) a un estado de entrega o en caso de otro acontecimiento definido previamente, se genera en el procesador (22b) un nuevo código de registro.

También es posible que se reciba un código de registro en el SHC (22) desde el servidor (30) de configuración central. El servidor (30) de configuración central puede generar un código de registro, por ejemplo siempre que se haya reiniciado el SHC (22). También es posible que el servidor (30) de configuración central pueda generar el código de registro, cuando se haya establecido una relación de propiedad. En este caso un código de registro anterior puede pasar a ser no válido y generarse un nuevo código de registro. También es posible que se cree un código de registro en el servidor (30) de configuración central siempre que un usuario se registre con el identificador que identifica unívocamente el SHC (22) en el servidor (30) de configuración central, para establecer la relación de propiedad. En ese momento puede generarse el código de registro en el servidor (30) de configuración y transmitirse a través de una conexión segura a través de Internet (28) y el encaminador (24) al SHC (22) para su visualización en el usuario. El usuario puede leer en ese momento el código de registro e introducirlo igualmente a través de Internet en el servidor (30) de configuración central y por consiguiente demostrar la propiedad del SHC (22) frente al servidor (30) de configuración central.

El código de registro también puede componerse de códigos aleatorios generados en el SHC (22) y el servidor (30) de configuración central. El código de registro puede ser o bien un código aleatorio, un código variable o un código que se extrae de una lista, que se conoce igualmente en el servidor (30) de configuración central. El código de registro determinado por medio del procesador (22b) se presenta visualmente en el dispositivo (22e) de visualización al usuario. Este código de registro representa por consiguiente un factor de propiedad, que se usa para la autorización del usuario para la configuración del SHC (22). Además de este factor de propiedad en el SHC (22) está impreso preferiblemente un número de serie, que el usuario también puede leer, pero que ya no se modifica.

La figura 3 muestra un servidor (30) de configuración central. El servidor (30) de configuración presenta una interfaz (30a) de comunicación y una segunda interfaz (30b) de comunicación. La primera interfaz (30a) de comunicación posibilita la comunicación del servidor (30) de configuración a través de Internet (28) con un SHC (22). La segunda interfaz (30b) de comunicación posibilita una comunicación del servidor (30) de configuración con un usuario por ejemplo a través de un ordenador (32a) personal o una pasarela (34) y un teléfono (32b) móvil.

Las interfaces (30a, 30b) de comunicación se controlan mediante un procesador (30e) previsto en el servidor (30) de configuración. El procesador (30e) controla además una unidad (30c) de comparación y una memoria (30d). En la memoria (30d) están almacenadas tuplas de identificador y código de registro. Por medio de esta tuplas es posible que un usuario pueda autorizarse de manera segura para el acceso al SHC (22). Las tuplas correspondientes se reciben a través de la interfaz (30a) de comunicación por el SHC (22), una vez que se haya reiniciado el SHC (22) o una vez que se haya generado en el SHC (22) un nuevo código de registro. Además de la tupla, al SHC (22) también está asociada una dirección de comunicación, a través de la que puede establecerse una conexión entre el SHC (22) y el servidor (30) de configuración.

Si a través de la interfaz (30b) de comunicación se desea un acceso a un SHC (22), entonces se verifica en primer lugar una autorización o la existencia de una relación de propiedad. Esto se realiza por medio del procesador (30e) y relaciones de propiedad almacenadas en la memoria (30d). Si no existe ninguna relación de propiedad, es decir para un nombre de usuario y una contraseña no está almacenado ningún SHC (22) asociado, entonces debe producirse una nueva autorización. Ésta se produce mediante la introducción de un código de registro y un identificador. El

procesador o la unidad (30) de comparación realiza una comparación de tuplas almacenadas en la memoria (30d) con las tuplas introducidas, y en caso de un resultado de comparación positivo se produce una autorización.

El desarrollo de la autorización se representa a continuación en las figuras 4 a 6.

La figura 4 muestra un diagrama de mensajes entre un usuario (36), un SHC (22) y un servidor (30) de configuración.

El servidor (30) de configuración puede estar dividido a nivel lógico y/o físico en tres servicios. Los servicios son a modo de ejemplo un servicio (31a) de registro, un servicio (31b) de personalización y un servicio (31c) de remisión. Sin embargo, también es posible que los servicios (31) estén agrupados en una unidad lógica y/o física.

Para la autorización de un usuario son necesarias las siguientes etapas.

En primer lugar, el usuario (36) realiza un reinicio (38) en el SHC (22). Alternativamente a la realización de un reinicio (38) también puede producirse otro acontecimiento, por ejemplo una expiración de tiempo, un nuevo inicio u otro acontecimiento. Una vez que se haya registrado en el SHC (22) el reinicio (38) o un acontecimiento equivalente, el procesador (22b) desencadena un programa para generar (40) un código de registro aleatorio en el procesador (22b). El código (40) de registro generado se visualiza (42) con ayuda del procesador (22b) en el dispositivo (22e) de visualización.

Además, el SHC (22) se registra (44) con ayuda de la interfaz (22a) de comunicación a través de la interfaz (30a) de comunicación en el servidor (30) de configuración central en particular en el servicio (31a) de registro. Con el registro (44), el SHC (22) transmite al servidor (30) de configuración al menos su número de serie. A continuación o al mismo tiempo el SHC (22) transmite (46) al servicio (31a) de registro del servidor (30) de configuración el código (40) de registro recién generado o el código de registro cifrado o un código *Hash* del código de registro. Por consiguiente, en el servidor (30) de configuración se conocen el identificador (número de serie) y el código de registro. En el servicio (31a) de registro o la memoria (30d) por medio del procesador (30e) se almacena la tupla formada por número de serie y código de registro.

Si un usuario (36) quiere habilitarse ahora para un acceso al SHC (22) a través del servidor (30) de configuración, accede (48) en primer lugar a una página de Internet del servicio (31b) de registro. A través de la página de Internet en el servicio (31b) de personalización el usuario introduce (50) el número de serie y el código de registro visualizado en el dispositivo (22e) de visualización. Con la introducción (50) del número de serie el usuario (36) garantiza que está en posesión del factor de conocimiento para la autorización. Con la introducción (50) del código de registro el usuario (36) garantiza que está en posesión del factor de propiedad. Ambos factores posibilitan una autorización segura del usuario (36), dado que sólo el propietario conoce el código de registro y varía de un propietario a otro.

El servicio (31b) de personalización comprueba (52) en el servicio (31a) de registro por medio de la unidad (30c) de comparación la tupla introducida por el usuario (36) con la tupla obtenida por el SHC (22) y almacenada en la memoria (30d). En caso de un resultado de comparación positivo, el servicio (31a) de registro informa (54) de la autorización satisfactoria al servicio (31b) de personalización. A continuación de esto, el servicio (31b) de personalización comunica al usuario (36) la autorización satisfactoria y se establece una relación de propiedad entre el usuario (36) y el SHC (22).

La relación de propiedad puede expresarse mediante un nombre de usuario y una contraseña. Por consiguiente, con ayuda del nombre de usuario y de la contraseña así como de una dirección de comunicación igualmente almacenada del SHC (22) resulta posible para el usuario (36) acceder a través del servidor (30) de configuración al SHC (22) con fines de configuración y de mando.

La cuenta de usuario o la relación de propiedad puede almacenarse en el SHC (22). Un almacenamiento (22) de este tipo se representa en la figura 4. Después de que el usuario haya establecido la relación de propiedad mediante la introducción en una cuenta de usuario de una contraseña de usuario, el servicio (31b) de personalización transmite (58) la información correspondiente al servicio (31a) de registro. El servicio (31a) de registro transmite (60) la información con respecto a la relación de propiedad junto con la cuenta de usuario al SHC (22). En el SHC (22) se almacena en la memoria (22c) la relación de propiedad.

Si el usuario quiere acceder ahora al SHC (22), se autentica frente al SHC (22) directamente tras la introducción (62) del nombre de usuario y de la contraseña. A continuación el usuario puede realizar interacciones (64a a 64f) en el SHC (22).

Si el usuario quiere realizar ahora una configuración del SHC (22), configuración que hace necesario que el usuario (36) utilice el servidor (30) de configuración, entonces el usuario (36) se autentica (66) frente al servicio (31c) de remisión del servidor (30) de configuración con ayuda del nombre de usuario y de la contraseña. Dado que en el caso representado en la figura 4 la cuenta de usuario está almacenada en el SHC (22), el servicio (31c) de remisión

comprueba (68) en el SHC (22) el nombre de usuario introducido junto con la contraseña. Si existe una autenticación correcta, entonces el SHC (22) autoriza (70) al usuario en el servicio (31c) de remisión. Tras una autorización satisfactoria, el usuario (36) puede realizar interacciones (72) de usuario en el servicio (31c) de remisión del servidor (30) de configuración, en particular modificaciones de configuración en el SHC (22). Las modificaciones de configuración se comunican (74) en el SHC (22).

La figura 5 muestra un desarrollo similar de un procedimiento, estando almacenadas sin embargo en este caso la relación de propiedad así como la cuenta de usuario en el servidor (30) de configuración central. Hasta la etapa (56) el procedimiento según la figura 5 corresponde al procedimiento según la figura 4.

Después de que el usuario haya creado la cuenta de usuario, se remite (76) el nombre de usuario junto con la contraseña desde el servicio (31) de personalización al servicio (31c) de remisión. En este caso, la cuenta de usuario se almacena en el servidor (30) de configuración o en la memoria (30d).

Si un usuario quiere acceder ahora directamente al SHC (22), entonces introduce (62) en primer lugar el nombre de usuario y la contraseña en el SHC (22). El SHC (22) comprueba la introducción al transmitir (78) los datos de cuenta de usuario introducidos al servicio (31c) de remisión. Si los datos introducidos coinciden con los datos almacenados en la memoria (30d), entonces el servicio (31c) de remisión autoriza al usuario y lo señaliza (80) al SHC (22). A continuación de esto, el usuario (36) puede realizar en el SHC (22) directamente acciones (64a-f) de usuario.

Si es necesaria una configuración a través del servidor (30) de configuración, entonces el usuario se registra (82) directamente en el servicio (31c) de remisión. Dado que la cuenta de usuario está almacenada en el servicio (31c) de remisión, directamente a continuación puede producirse una interacción (84) de usuario, que en el caso de una autenticación satisfactoria conduce a una remisión (86) de las modificaciones de configuración al SHC.

La figura 6 muestra el desarrollo de un procedimiento mostrado en las figuras 4 y 5. Las etapas 38 a 56 corresponden a las de las figuras 4 y 5.

En el procedimiento mostrado en la figura 6 se almacena la relación de propiedad por un lado en el servidor (30) de configuración y en paralelo a esto también en el SHC (22). Esto significa que se realizan las etapas (76) según la figura 5 y (58 y 60) según la figura 4, de modo que mediante la etapa (76) se almacena la cuenta de usuario en el servicio (31c) de remisión o la memoria (30d) del servidor (30) de configuración y en paralelo mediante las etapas (58 a 60) se almacena la cuenta de usuario en el SHC (22). Por consiguiente, en el caso de una interacción de usuario directamente en el SHC es posible una autenticación (62) directamente en el SHC (22). Si es necesaria una configuración a través del servidor (30), pueden realizarse las etapas (82 a 86) según la figura 5.

REIVINDICACIONES

1. Procedimiento para generar una autorización de acceso a un servidor (22) de domótica por medio de un servidor (30) de configuración central a través de una red (28) de área amplia, que comprende:

- almacenar al menos una primera tupla formada por un identificador que identifica unívocamente el servidor (22) de domótica y un código de registro en el servidor (30) de configuración central,

- recibir una segunda tupla formada por al menos un identificador y un código de registro en el servidor (30) de configuración central de un usuario,

- comparar la primera tupla con la segunda tupla mediante el servidor de configuración central,

- almacenar una relación de propiedad entre el usuario y el servidor (22) de domótica en caso de un resultado de comparación positivo, de tal manera que por medio de la relación de propiedad se genera una autorización de acceso al servidor (22) de domótica a través de la red (28) de área amplia.

2. Procedimiento según la reivindicación 1, caracterizado porque el código de registro es un código aleatorio generado en el servidor (22) de domótica y porque la primera tupla se transmite desde el servidor (22) de domótica al servidor (30) de configuración central a través de la red (28) de área amplia, o porque el código de registro es un código aleatorio generado en el servidor (30) de configuración central y se transmite desde el servidor (30) de configuración central al servidor (22) de domótica a través de la red (28) de área amplia.

3. Procedimiento según la reivindicación 1 ó 2, caracterizado porque el código de registro se visualiza en un dispositivo (22e) de visualización en el servidor (22) de domótica.

4. Procedimiento según una de las reivindicaciones 1 a 3, caracterizado porque en cada caso se genera un nuevo código de registro cada vez que se reinicia el servidor (22) de domótica.

5. Procedimiento según una de las reivindicaciones 1 a 4, caracterizado porque al código de registro está asociado un periodo de validez y porque tras la expiración del periodo de validez es imposible generar una autorización de acceso con el código de registro caducado o porque el código de registro se marca como no válido tras un único uso.

6. Procedimiento según una de las reivindicaciones 1 a 5, caracterizado porque con ayuda de una autorización de acceso se crea una cuenta de usuario, estando asociadas a una cuenta de usuario restricciones de acceso al servidor (22) de domótica.

7. Procedimiento según la reivindicación 6, caracterizado porque la cuenta de usuario se almacena en el servidor (22) de domótica y/o el servidor (30) de configuración central.

8. Procedimiento según una de las reivindicaciones 1 a 4, caracterizado porque el identificador es un número de serie del servidor (22) de domótica.

9. Procedimiento según la reivindicación 1, caracterizado porque el código de registro es un código variable generado en el servidor (22) de domótica.

10. Servidor de domótica con

- un procesador (22b),

- una primera interfaz (22a) de comunicación para la comunicación a través de una red (28) de área amplia con un servidor (30) de configuración central,

- una segunda interfaz (22a) de comunicación para la comunicación con aparatos (2, 12) locales, y

- una unidad (22e) de visualización,

caracterizado

- porque el procesador (22b) activa la unidad (22e) de visualización para visualizar un código de registro, y

- porque el procesador (22b) para configurar una autorización de acceso a través de la red (28) de área amplia al servidor (22) de domótica activa la primera interfaz (22a) de comunicación para emitir el código de

registro junto con un identificador que identifica unívocamente el servidor (22) de domótica al servidor (30) de configuración central o para recibir el código de registro del servidor (30) de configuración central.

11. Servidor de domótica según la reivindicación 10, caracterizado porque en cada caso se visualiza un nuevo código de registro cada vez que se reinicia el servidor (22) de domótica.

12. Servidor de configuración central con:

- una memoria (30d) configurada para almacenar al menos una primera tupla formada por un identificador que identifica unívocamente el servidor (22) de domótica y un código de registro en el servidor (30) de configuración central,

- una interfaz (30b) de comunicación configurada para recibir una segunda tupla formada por al menos un identificador y un código de registro en el servidor de configuración central de un usuario,

- un procesador (30e) configurado para comparar la primera tupla con la segunda tupla, y

- posibilitando la interfaz (30b) de comunicación con ayuda de una relación de propiedad entre el usuario y el servidor (22) de domótica un acceso al servidor de domótica a través de la red de área amplia.

13. Sistema con un servidor de configuración central según la reivindicación 12 y un servidor de domótica según la reivindicación 10.

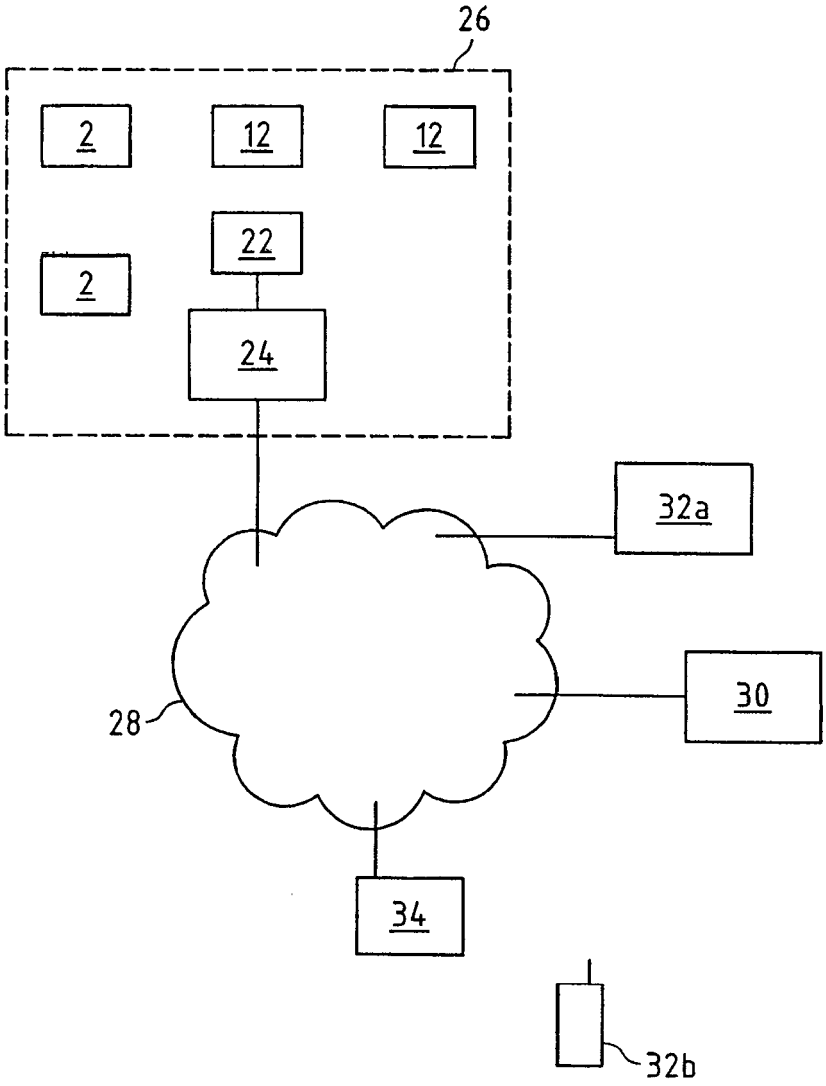

Fig.1

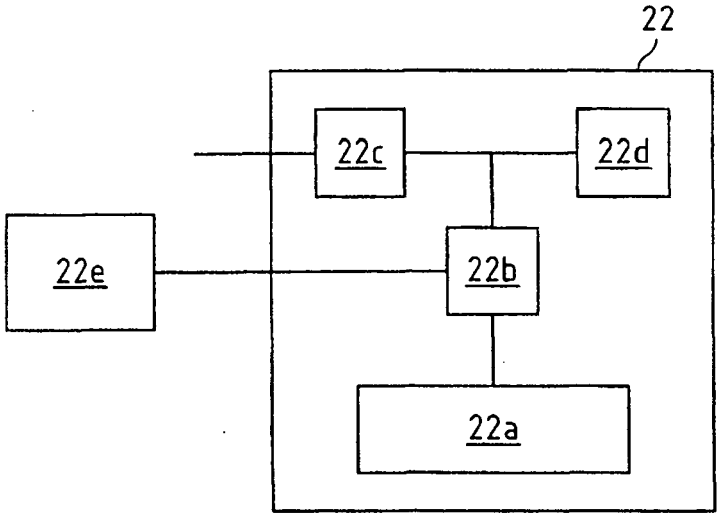

Fig.2

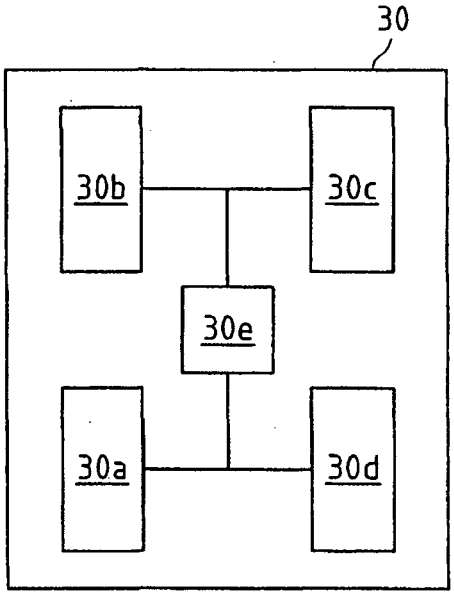

Fig.3

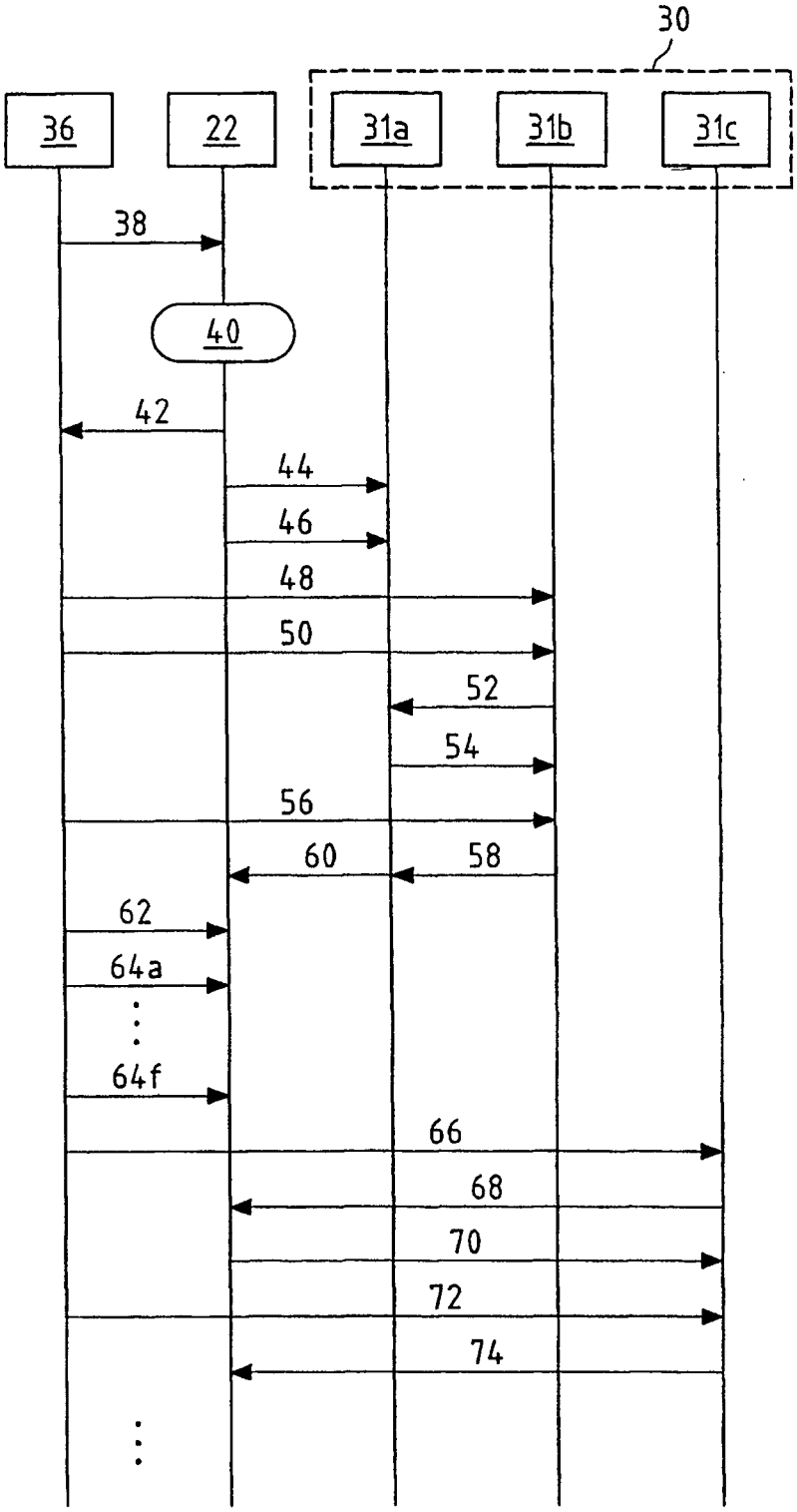
30
36
22
31a
31b
31c
38
40
42
44
46
48
50
52
54
56
60
58
62
64a
64f
66
68
70
72
74

Fig.4

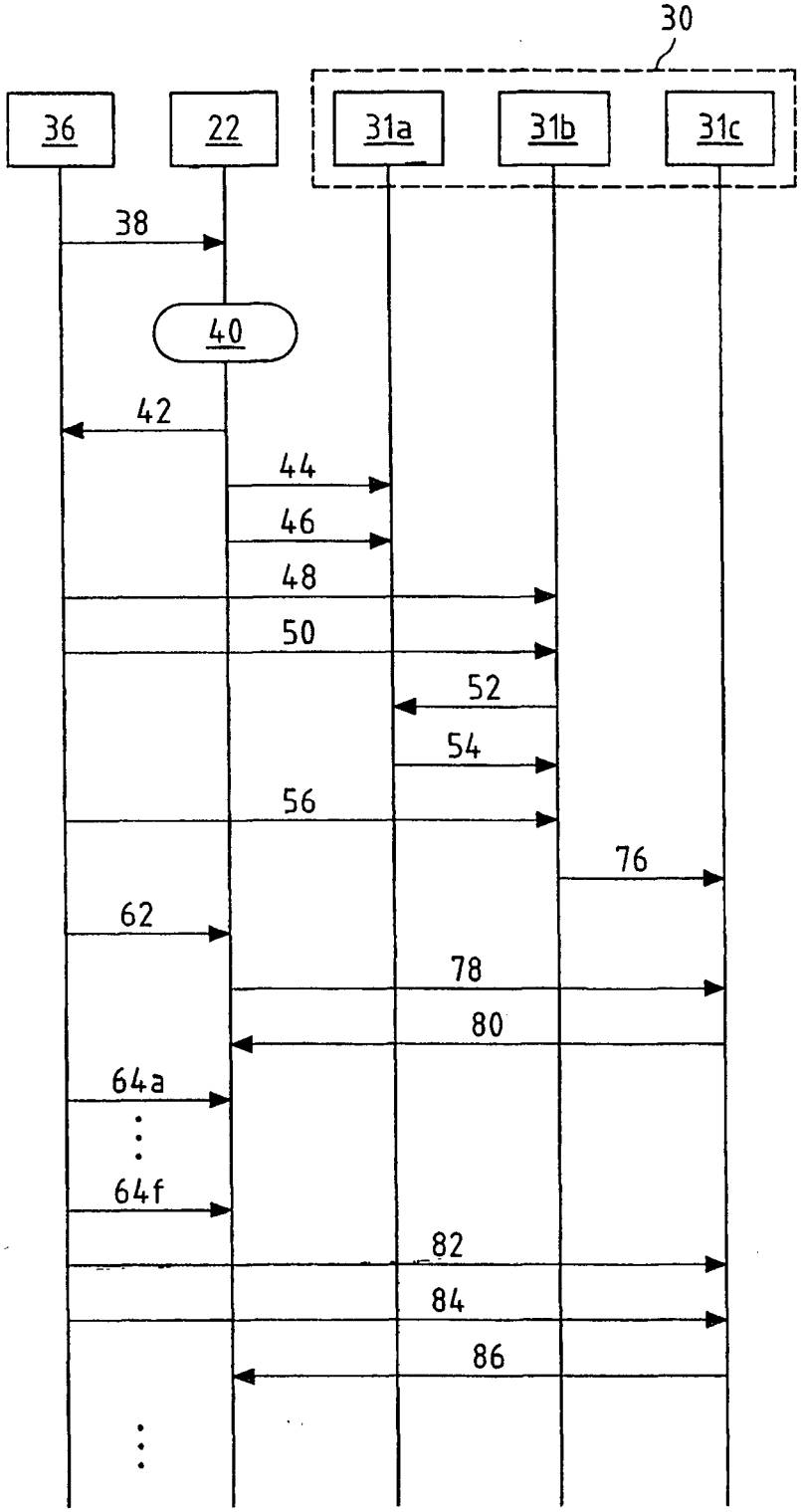
30
36
22
31a
31b
31c
38
40
42
44
46
48
50
52
54
56
76
62
78
80
64a
64f
82
84
86

Fig.5

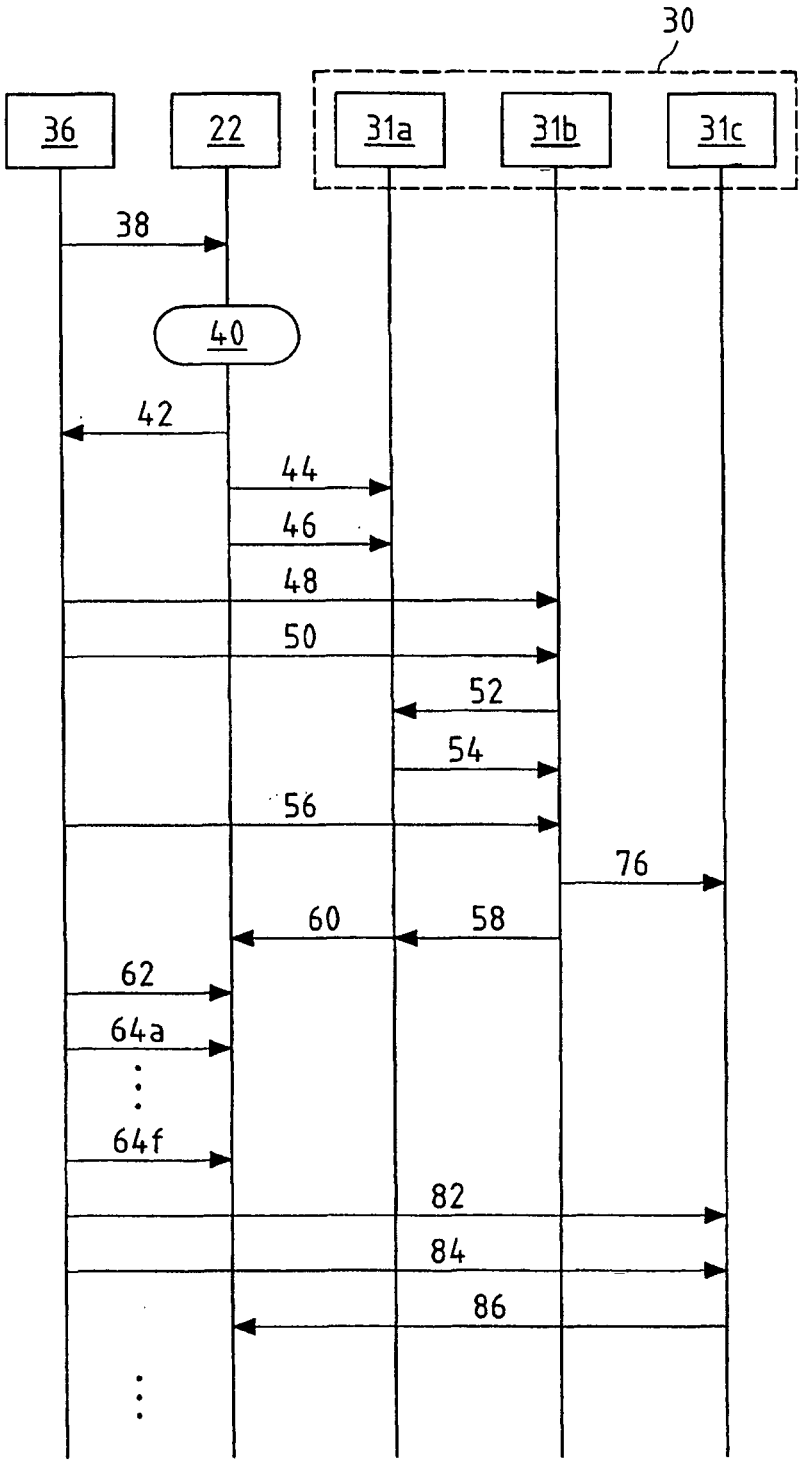
30
36
22
31a
31b
31c
38
40
42
44
46
48
50
52
54
56
76
60
58
62
64a
64f
82
84
86

Fig.6